UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/532,193	04/21/2005	Alain Durand	PF030167	8417

24498 7590 11/05/2010

Robert D. Shedd, Patent Operations
THOMSON Licensing LLC
P.O. Box 5312
Princeton, NJ 08543-5312

EXAMINER	
VAUGHAN, MICHAEL R	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
11/05/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/532,193	DURAND ET AL.	
	Examiner	Art Unit	
	MICHAEL R. VAUGHAN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 August 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

In view of the Appeal Brief filed on 8/18/10, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes et al. "Handbook of Applied Cryptography, PASSAGE." Handbook of Applied Cryptography, CRC Press Series on Discrete Mathematics and its Applications, Boca Raton, FI, CRC Press, US, 1997, pages 497-553, hereinafter Menezes, in view of USP Application Publication 2005/0025091 to Patel et al., hereinafter Patel.

As per claim 1, Menezes teaches a method for encrypting data in a communication network comprising a device of a first type [B] containing:

a first symmetric key [session key, k] for encrypting the data to be sent to a device of a second type [A] connected to the network (pg. 503) wherein said second type of device is a different device type from said device of a first type; and

an encrypted first symmetric key which generated from the encryption of said first symmetric key with a second symmetric network key [$_{KAT}$] known only by at least one device of a second type connected to said network [session key encrypted by key $E_{KAT}(k)$; pg. 503];

the method comprising the steps that consist, for the device of a first type [note that this limitation does not require the device of a first type to actual perform any of these steps because "for the device" does not mean "by the device"], in:

(a) generating a random number [Nb]; pg. 503];

(c) encrypting the data to be transmitted with the new symmetric key [data is encrypted with k; pg. 503]; and

(d) transmitting to a device of a second type [A], via said network:

the data encrypted with the new symmetric key [session key, k, is used to encrypt the data, therefore it is inherent data will be encrypted; pgs 497-503]

the random number [Nb; pg. 503, step 4]; and

said encrypted first symmetric key [$E_{KAT}(k)$] (pg. 503, protocol message 2). Menezes is silent in disclosing computing a new symmetric key as a function of the first symmetric key and said random number. Menezes teaches the session keys needs to be updated and are a function of a random number but does not explicitly teach incorporating a previous session key into the function and a weakness of the Needham-Schroeder protocol is the freshness of 'k'. Patel teaches one way of updating a session key is by hashing the session key with a random number to generate a new session key (0059). It is well known that session keys needs to be updated frequently to secure the system. Updating the key as taught by Patel also increases the security by not having to send the new key across the channel. Only the random number need by sent and both parties can derive the new key. This would also alleviate having to contact the trusted server for another session key. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Patel into the system of Menezes because it would provide a mechanism for securely updating the session keys.

As per claim 2, Menezes teaches the function used to compute the new symmetric key is a one-way derivation function [hk; pg. 499].

As per claim 3, Menezes teaches the function is a hash or encryption function hk; pg. 499].

As per claim 4, Menezes teaches the device of a second type [A] that receives data transmitted at step (d), in:

(e) decrypting, with the second symmetric network key, the encrypted first symmetric key as to produce encryption of the first symmetric key [A uses the K_{AT} to decrypt E_{KAT} to obtain k; pg. 503];

(f) determining, based on the first symmetric key obtained at step (e) and on said random number, the new symmetric key [pg. 498]; and

(g) decrypting the data received with the new symmetric key [session key is used to encrypt the data, therefore it is inherent data will be encrypted; pgs 497-499].

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431